GE HealthCare

Voluson **Expert 22**

Безопасность и конфиденциальность

Границы возможного в ваших руках

С развитием цифровых возможностей, включая технологию беспроводного соединения и программное обеспечение в здравоохранении, вероятность возникновения киберугроз и/или несанкционированного доступа к данным неотвратимо возрастает. Ультразвуковые устройства являются компьютерной системой и могут быть уязвимы для угроз кибербезопасности, что может отразиться на эффективности и защите данных такого устройства.

Приоритетной задачей компании GE HealthCare является обеспечение безопасности и конфиденциальности данных ваших пациентов. Мы прилагаем все усилия, чтобы ультразвуковые системы Voluson™ работали с использованием новейших и наиболее передовых политик и технологий безопасности, при этом сохраняя гибкость, необходимую для эффективного управления вашей клиникой.

yes@medsyst.ru
8 800 500 9093

Medsyst.ru

YouTube

КИБЕРБЕЗОПАСНОСТЬ — ЭТО БОЛЬШЕ, ЧЕМ АНТИВИРУСНАЯ ЗАЩИТА

Разработка ультразвуковой системы с максимальным уровнем безопасности

Компания GE HealthCare разработала стратегическую программу DEPS (Проектирование с учетом конфиденциальности и безопасности), которая используется при развитии наших продуктов. Процесс проектирования начинается с оценки риска конфиденциальности и безопасности и предоставления рекомендаций группе разработчиков ультразвуковой системы. Ультразвуковые системы Voluson включают в себя следующие элементы конструкции, обеспечивающие вашу защиту с самого начала эксплуатации:

- Операционная система Windows® 10 IoT Enterprise с возможностью установки последних обновлений для системы безопасности по мере их получения от Microsoft®. Это обновление может быть выполнено только после инженерной оценки и испытаний на совместимость с системой
- Основные программные компоненты ультразвуковых систем Voluson, включая операционную систему Microsoft Windows 10 IoT Enterprise, настраиваются с использованием рекомендованных стандартов, таких как программы по кибербезопасности DISA (Агентство оборонных информационных систем), STIG (Руководства по технической реализации мер обеспечения безопасности), NIST (Национальный институт стандартов и технологий) и передовых практик Центра интернет-безопасности (CIS)
- Встроенные в операционную систему программные службы, которые не требуются для работы на ультразвуковой системе, удалены или отключены
- Неиспользуемые для передачи данных сетевые порты отключены для минимизации риска заражения
- Защита от атак с USB-носителя путем сканирования USB-носителя на наличие угроз безопасности непосредственно при его подключении и отключения любых функций автозапуска
- Предотвращение импорта/экспорта данных на ультразвуковой системе путем отключения накопительных устройств на портах USB
- В качестве средства антивирусной защиты применяется ведение списков разрешенных приложений (whitelisting) — ограничение числа программ запускаемых на системе (только заранее идентифицированные и одобренныеи продукты). Для защиты ультразвуковой системы не запускаются неизвестные, потенциально вредоносные программы
- Преимуществом такой крупной компании, как GE HealthCare, является наличие надежной централизованной службы безопасности, которая постоянно отслеживает новые угрозы и взаимодействует с инженерами Voluson по разработке и внедрению дополнительных обновлений безопасности по мере необходимости

Примечание: Voluson Expert 22 — Волюсон Эксперт 22.

Материал предназначен исключительно для медицинских и фармацевтических работников.

Поддержание конфиденциальности и безопасности данных пациентов

Защита систем от вредоносных программ или других кибератак является одним из аспектов безопасности системы, но также важно защитить и локально хранящуюся информацию от кражи или повреждения. Именно тогда начинают действовать меры по защите данных.

Безопасный совместный доступ

- Локально хранящаяся информация о пациентах может быть защищена с помощью шифрования жесткого диска — шифрование по стандарту AES с 256-битной длиной ключа
- В ультразвуковых системах Voluson используется передача данных с шифрованием по стандарту DICOM® (по протоколу TLS). Протокол TLS — это криптографический протокол, обеспечивающий защищенный обмен данными. Благодаря такому шифрованию передаваемые по вашим сетям данные невозможно перехватить, считать и изменить во время передачи в ViewPoint™, систему PACS, МИС и т. д.*

Управление пользователями

- Простое управление доступом к ультразвуковой системе для нескольких пользователей с индивидуальными учетными записями — определение настраиваемых уровней доступа к функционалу системы в зависимости от потребностей пользователя
- Параметрами (учетными данными) доступа пользователей можно управлять удаленно с помощью интерфейса через протокол LDAP (облегченный протокол доступа к каталогу), предназначенного, в частности, для использования в крупных учреждениях
- Система Voluson может отслеживать и регистрировать любые действия, связанные с безопасностью, включая действия по управлению пользователями, бездействие системы, события входа/выхода, а также обработку данных и изменения конфигурации, создавая журнал регистрации событий и журнал использования

* Проверьте PACS-систему и медицинскую информационную систему на наличие шифрования TLS.

Представленные ультразвуковые системы зарегистрированы на территории РФ как «Система ультразвуковая диагностическая медицинская с принадлежностями варианты исполнения Voluson Expert 18, Voluson Expert 20, Voluson Expert 22».

Voluson Expert — Волюсон Эксперт

ViewPoint зарегистрирован на территории РФ как «Программное обеспечение для хранения, обработки и анализа ультразвуковых данных ViewPoint с принадлежностями».

GE HealthCare

yes@medsyst.ru
8 800 500 9093

Medsyst.ru

YouTube